

reading out both a preceding biometric record and preceding associated spatial position data of a preceding user identification process which precedes the current user identification process;

comparing the biometric record currently acquired and the associated spatial position data with the preceding biometric record and the associated spatial position data read out; and

rejecting the identification of the user if there is a defined degree of correspondence between the biometric record currently acquired and the preceding biometric record, and the spatial position data currently acquired is within a defined tolerance range from the preceding spatial position data.

18. A method for biometric identification of a user as claimed in Claim 17, wherein the tolerance range is less than 100 μm .

19. A method for biometric identification of a user as claimed in Claim 17, wherein the tolerance range is approximately 50 μm .

20. A method for biometric identification of a user as claim in Claim 17, the method further comprising the steps of:

determining a mean value of positions of a plurality of individual features of the biometric record in each user identification process; and

using the mean values of two successive user identification processes in the step of comparing.

21. A method for biometric identification of a user as claimed in Claim 20, wherein the tolerance range is less than 50 μm .

22. A method for biometric identification of a user as claimed in Claim 20, wherein the tolerance range is between 10 μm and 20 μm .

23. A method for biometric identification of a user as claimed in Claim 17, wherein the biometric record is fingerprint data.

24. A method for biometric identification of a user as claimed in Claim 23, the method further comprising the step of:

determining, as the spatial position data, coordinates of at least one of branches and minuscules of the fingerprint on a contact area.

25. A method for biometric identification of a user as claimed in Claim 17, the method further comprising the steps of

deleting, after a user identification process has ended, the stored biometric record in the associated spatial position data of the preceding identification process; and

overriding the previously stored biometric record and the associated spatial position data of the preceding identification process with the biometric record and the associated spatial position data of the current identification process.

26. An apparatus for biometric identification of a user, comprising;
a device for acquiring, in a current user identification process, both a biometric record of the user and associated spatial position data of the biometric record relative to a reference position;

a memory for storing both the biometric record and the associated spatial position data; and

a comparison device for comparing the biometric record currently acquired and the associated spatial position data with a preceding biometric record and preceding associated spatial position data of a preceding user identification process, and for rejecting the identification of the user if there is a defined degree of correspondence between the biometric record currently acquired and the preceding biometric record, and the spatial position data currently acquired is within a defined tolerance range from the preceding spatial identification data.

27. An apparatus for biometric identification of a user as claimed in Claim 26, further comprising:

an output device for outputting a result of the user identification process.

28. An apparatus for biometric identification of a user as claimed in Claim 26, wherein the tolerance range is less than 100 μm .

29. An apparatus for biometric identification of a user as claimed in Claim 26, wherein the tolerance range is approximately 50 μm .

30. An apparatus for biometric identification of a user as claimed in Claim 26, further comprising:

a device for calculating a mean value of positions of a plurality of individual features of the biometric record in each user identification process, wherein the comparison device compares the mean values of two successive user identification processes.